BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi jaringan komputer berkembang dengan sangat pesat, Perkembangan ini diawali oleh munculnya *internet* sebagai media informasi yang dapat diakses dengan menggunakan komputer yang terkoneksi ke berbagai belahan dunia sehingga pengaksesan informasi, proses komunikasi, dan pertukaran data dapat dilakukan di mana saja dengan mudah. Namun, akibat dari perkembangan teknologi tersebut seperti terhubungnya *LAN* atau komputer ke *internet* membuka potensi adanya lubang keamanan (*security hole*), Hal ini dapat menjadi masalah besar apabila tidak ditangani dengan benar karena dengan tereksploitasinya lubang keamanan, maka pengguna yang tidak berhak seperti *hacker* dan *intruder* (penyusup) dapat dengan mudah melakukan kejahatan-kejahatan dalam dunia cyber yang dikenal dengan Cyber *Crime*, seperti *sniffing, spoofing, DoS attack,* dan lain sebagainya yang dapat dikategorikan sebagai kejahatan dalam dunia maya.

Website merupakan salah satu layanan informasi yang banyak diakses oleh pengguna *internet* di dunia. Pada dasarnya terdapat 4 (empat) elemen dasar dari sebuah *website* yaitu: *browser, server, URL,* dan *pages. Webserver* berisi *web pages,* yang di dalamnya mengandung informasi atau dokumen yang ingin disebarluaskan atau diperlukan oleh para pengguna. Perkembangan teknologi membuat *website* menjadi alat berbagi informasi secara global. *Website* sendiri

terhubung ke *webserver*. Sejak beberapa tahun terakhir ini keamanan merupakan pokok persoalan utama. Banyak diberitakan mengenai penyusupan di *website* dan perusahaan atau perusakan dan penghilangan aset perusahaan yang dalam bentuk digital. *Webserver* seringkali menjadi target dari berbagai jenis serangan baik yang sifatnya minor maupun major sehingga berakibat fatal. Akan tetapi, adakalanya *website* dijadikan pintu oleh peretas (*hacker*) untuk menembus *webserver* bahkan sampai ke *root* untuk kesenangan bahkan dengan sengaja menyerang *website* tersebut. Beberapa contoh eksploitasi pada *webserver* yang sering terjadi adalah antara lain melakukan perubahan tampilan (*deface*), perubahan data pada *server*, penyadapan informasi, *DoS attack*, *ping flood*, dan sebagainya.

Keamanan *server website* biasanya merupakan masalah dari seorang administrator. Seorang administrator bertugas untuk mengawasi dan melakukan tindakan preventif ketika terjadi aksi penyusupan dan serangan. Masalah timbul ketika sang adminstrator sedang tidak berada pada posisi siap sedia, misalnya sakit, berada diluar jam kerja, atau adanya kepentingan mendadak. Sedangkan, serangan terhadap *server* bisa terjadi kapan saja. Dengan memasang *server website* di sistem berarti membuka akses (meskipun secara terbatas) pada orang luar. Apabila *server* terhubung ke *internet* dan apabila *server website* disiapkan untuk publik, maka *webserver* dan *database server* bagaikan jantung dan otak dari organisme *internet*. Dua komponen ini menjadi komponen pokok dari sebuah aplikasi internet yang tangguh dan tepatlah keduanya menjadi target *hacker*. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang dapat diterima.

Dalam sebuah *survei* oleh *Computer Security Institut* (2009) terhadap macam-macam serangan yang terjadi pada jaringan *internet* dan komputer, serangan *Denial of Service (Dos)* menempati peringkat 3 (tiga), sedangkan pada tahun 2010/2011, serangan *Denial of Service (Dos)* menempati peringkat 4 (empat). Dilihat dari *survey* tersebut, *Dos* masih menjadi ancaman untuk merusak atau melumpuhkan sebuah *host* atau *server*.

Nurwenda, Irawan, dan Irzaman (2004) mengemukakan bahwa *Denial of Service (DoS) attack* adalah ancaman yang serius untuk jaringan komputer seperti *Local Area Network* (*LAN*), dan internet. *DoS attack* dapat mengkonsumsi *memory, CPU,* dan sumber daya jaringan, serta dapat menyebabkan kerusakan atau *shutdown* terhadap sumber daya operasi yang berada di dalam serangan. Secara umum serangan *DoS* adalah membanjiri suatu jaringan dengan lalu lintas palsu sedemikian sehingga para pemakai sah tidak mungkin mampu untuk berkomunikasi.

Keamanan jaringan merupakan aspek pertahanan suatu jaringan komputer. *Firewall* merupakan salah satu sistem keamanan yang berfungsi untuk mencegah penggunaan yang tidak sah serta pembatasan akses tertentu pada suatu perangkat. Penggunaan *firewall system* dapat meningkatkan efisiensi dalam perancangan jaringan komputer. Paulan, Herdiansyah, dan Santi (2012) menerapkan *Iptables* sebagai *firewall* pada *server* untuk melakukan pemblokiran terhadap serangan *DoS*. Hasil penelitian tersebut menunjukkan bahwa serangan *flooding* ke *port* 80 setelah di-*filter* dengan *firewall* tidak berhasil dikarenakan sudah diterapkan pencegahan dan pemblokiran dengan *Iptables*.

Keamanan *web*, sangat erat kaitannya dengan jaringan karena untuk mengakses sebuah *website* pasti dibutuhkan koneksi jaringan. Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi, namun masalah keamanan ini seringkali kurang diperhatikan oleh para pemilik dan pengelola sistem informasi sehingga memungkinkan terjadinya resiko yang cukup signifikan. Sebagai contoh, dalam suatu persaingan bisnis dalam dunia maya, dapat memungkinkan terjadinya suatu penyerangan terhadap *webserver* yang kemudian akan menimbulkan kerugian bagi pemilik dimana *website* yang diserang menjadi *down* atau tidak dapat diakses oleh *client* sehingga dapat memberikan kontribusi bagi para pesaing bisnis lainnya.

Berdasarkan latar belakang di atas, maka akan dilakukan penelitian dengan judul "**ANALISA DAN PERANCANGAN SISTEM KEAMANAN JARINGAN *WEBSERVER* DARI SERANGAN *DENIAL OF SERVICE* (*DOS*) DENGAN MENGGUNAKAN METODE *PENETRATION TEST***".

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka perumusan masalah dalam penelitian ini, yaitu.

1. Bagaimana menganalisa serta menemukan kelemahan pada *webserver* dengan melakukan serangan *Denial of Service* (*DoS*).
2. Bagaimana implementasi suatu keamanan *webserver* dengan *Iptables* dalam mencegah serangan *Denial of Service* (*DoS*).

1.3 Batasan Masalah

Dalam penelitian ini, penulis akan membatasi masalah sebagai berikut:

1. Metode pengujian sistem keamanan *webserver* dengan menggunakan *penetration testing*
2. Melakukan serangan dengan menggunakan *Denial Of Service* (*DoS*)
3. Perancangan sistem keamanan *webserver* berbasis *iptables*
4. Tools *denial of service* (*DoS*) yang digunakan berupa aplikasi *DoSHTTP* 2.5.1 dan *GoodBye* 3.0

1.4 Tujuan Penelitian

Untuk mengetahui dan mempelajari peranan serta cara kerja dari *Iptables* terhadap proteksi akses jaringan internet *webserver* dan membangun suatu sistem keamanan *webserver* dengan menggunakan *Iptables* sebagai *firewall*.

1.5 Manfaat Penelitian

1. Mempermudah administrator jaringan dalam melakukan pencegahan adanya serangan *Denial of Service* (*DoS*)
2. Menambah wawasan penulis tentang teknologi jaringan *webserver*, khususnya sistem keamanan *webserver* berbasis *Iptables.*
3. Memberikan kontribusi pemikiran bagi manajemen perusahaan maupun individual dalam mengambil keputusan berkenaan dengan teknologi jaringan komputer khususnya sistem keamanan jaringan *webserver* dengan menggunakan *iptables*

1.6 Sistematika Penulisan

Penelitian ini dibagi menjadi lima bab dengan sistematika penulisan penelitian sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan secara ringkas mengenai latar belakang penelitian, perumusan masalah, pembatasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menjelaskan landasan teori yang berhubungan dengan topik pembahasan penelitian ini, penelitian terdahulu dan model yang mendasari penelitian.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini menguraikan tentang rancangan yang digunakan dalam penelitian, terdiri dari Alur Penelitian, Analisis Permasalahan, dan Perancangan Sistem.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini menguraikan gambaran umum objek penelitian, membahas hasil analisis penelitian dan pengujian serta temuan-temuan mengenai analisis keamanan *webserver* dari serangan *DoS* dengan menggunakan *Iptables* sebagai *firewall*

BAB V KESIMPULAN DAN SARAN

Bab ini memuat kesimpulan, keterbatasan, dan saran untuk peneliti di masa yang akan datang dan diharapkan dapat memberikan manfaat.